Volume I, Appendix E – Table of Contents

E. Network Security E-1

E.1 Purpose E-1

E.2 DON Information Protection Requirements E-2

E.2.1 Requirements Areas E-2

E.2.2 Protection Mechanisms E-3

E.2.3 Protection Dimensions E-3

E.3 Defense in Depth Approach E-3

E.4 Mechanisms E-5

E.4.1 Zone 4 Mechanisms E-5

E.4.2 Zone 3 Mechanisms E-8

E.4.3 Zone 2 Mechanisms E-9

E.4.4 Zone 1 Mechanisms E-10

E.5 Infrastructure Security Components E-11

E.5.1 Infrastructure Mechanism – Secure Domain Name System E-11

E.5.2 Infrastructure Mechanism – Public Key Infrastructure E-11

E.5.3 Infrastructure Mechanism – Network Management Security E-11

E.5.4 Infrastructure Mechanisms – Network Security Configuration Management E-11

E.5.5 Infrastructure Mechanisms – ATM-level Security E-12

E.5.6 Infrastructure Mechanisms – IP Security E-12

This page intentionally left blank.

E. Network Security

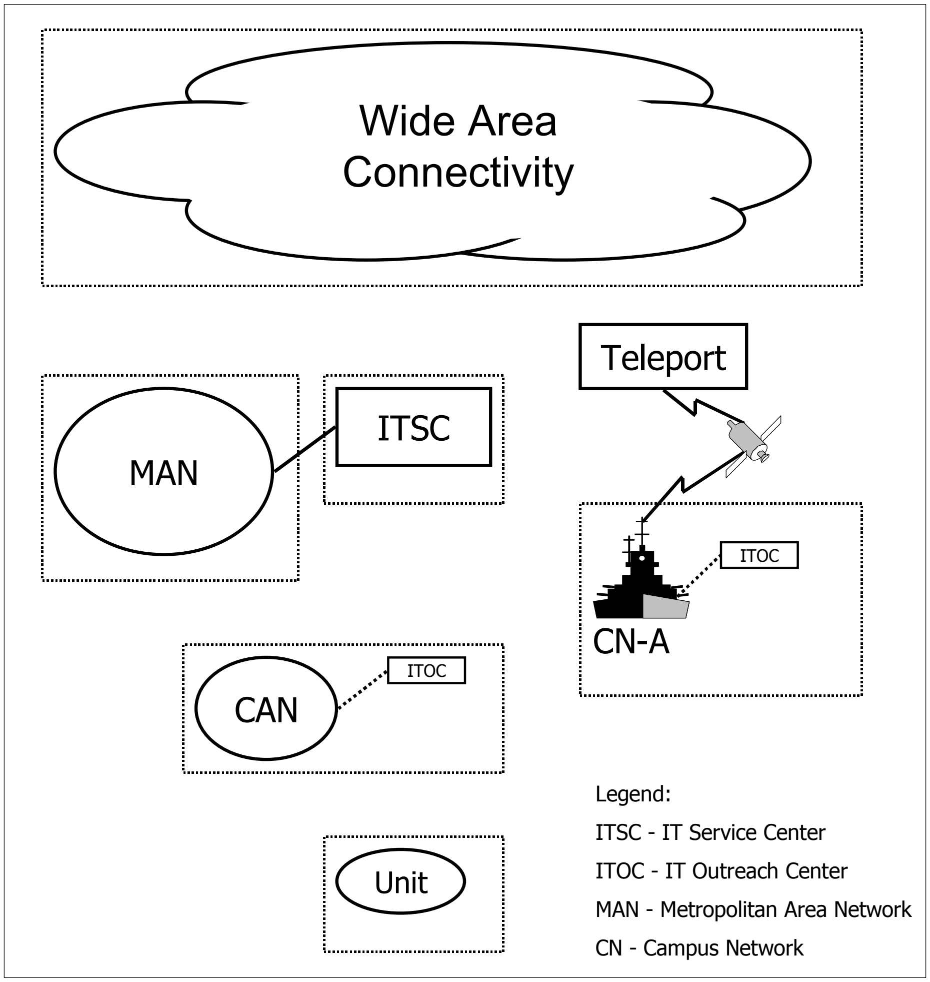


Figure E-1. High Level Components of ITI Architecture

E.1 Purpose

The components of the ITI architecture shown in Figure E-1 were addressed in their respective templates in the preceding appendices. Each template included specific security mechanisms that were appropriate to that level of the ITI infrastructure. Security was integrated into each template to ensure a clear definition of the placement and configuration of the security mechanisms. In this final appendix, security is discussed in aggregate, describing how all of these security mechanisms combine into a “Defense in Depth” security system. ITI Security is addressed in the following three segments:

- The information protection requirements that must be addressed in the Navy and Marine Corps

- The significant infrastructure mechanisms that are used to provide protection at specific points in the technology infrastructure
- A DON defense in depth strategy used to frame the Navy and Marine Corps information protection strategy

E.2 DON Information Protection Requirements

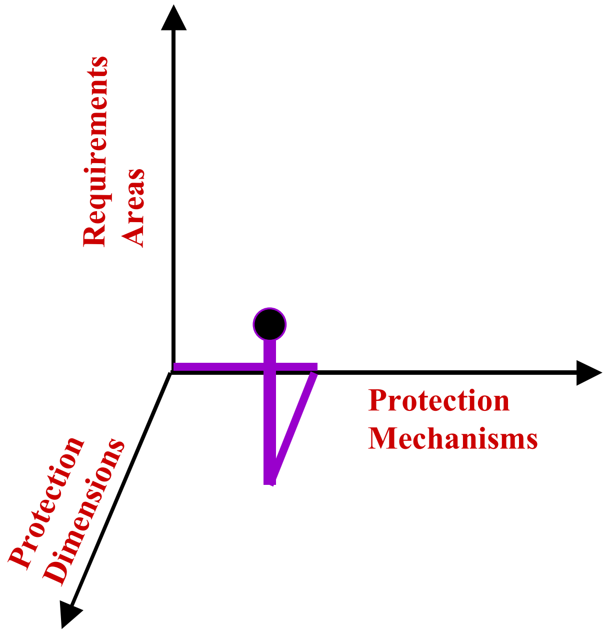


Figure E-1. Information Protection Summary

Figure E-1 depicts the interrelationship of the requirements, mechanisms, and dimensions in a three-axis model. There are five protection requirements areas, six protection mechanisms, and three protection dimensions. The simplified model shown in Figure E-1 masks the innumerable intersections of the three axes that produce nearly 100 instances of specific information protection requirements. The information protection requirements must be defined for each of the requirements intersections.

E.2.1 Requirements Areas

As DON IT regionalization efforts proceed, system designers must ensure that the resulting systems meet certain information protection requirements. The generic information protection classes of requirements for DON information systems are:

- **Confidentiality** – the protection of classified and sensitive but unclassified (SBU) information from unauthorized disclosure
- **Integrity** – the protection of information and information system resources from unauthorized, undetected modification
- **Availability** – the assurance that authorized users will have reliable and timely access to required resources (including information, system services, communication services, etc.)

- **Authenticity** – the ability to determine if information was created or modified by an authorized entity
- **Non-repudiation** – the ability to provide non-forgeable proof of a data originator's identity and non-forgeable proof of data receipt

E.2.2 Protection Mechanisms

The following broad categories of information protection mechanisms satisfy the information protection requirements:

- **Encryption –** convert understandable information into unintelligible data for storage and transport in harmful environments and restore this information (decryption) to authorized users
- **Access Control** – control access to system data and resources based on a user's identity or operational role
- **User Identification and Authentication (I&A) –** securely determine a user's identity or operational role
- **Malicious Content Detection –** examine incoming data to detect and block malicious content (e.g., viruses)
- **Audit –** record security-relevant events in a protected form (for use in non-real time event reconstruction and in real time intrusion detection)
- **Physical and Environmental Controls** – physically protect and provide for continuity of operations for system components relating to policies, procedures, and mechanisms

E.2.3 Protection Dimensions

To achieve information protection over the DON enterprise, the information architecture is categorized in dimensions that must be protected. The top-level dimensions are listed from more general to specific:

- **Information System** – the actual infrastructure that must be protected against unauthorized intrusion and denial of service
- **Information Domain –** communities of interest (CoIs) within the infrastructure must be afforded freedom to move and process information within a virtual enclave that provides protection
- **Information Content –** information packages themselves must be protected against unauthorized access by untrusted users both while in transit and in storage

E.3 Defense in Depth Approach

Defense in depth is the preferred approach for information protection for the Naval enterprise as regionalization efforts proceed. In defense in depth, information protection mechanisms are applied in multiple, complementary, and redundant locations in a system architecture. The system satisfies its information protection policy while maximizing resistance to attack and minimizing the potential that a flaw in a single security mechanism will lead to a security compromise. Additionally, defense in depth allows for varying levels of permeability in the information protection architecture. For example, more strict security restrictions can be placed on the flow of information from the Internet to a Naval regional MAN than the restrictions placed on the flow of information between two Naval regional MANs.

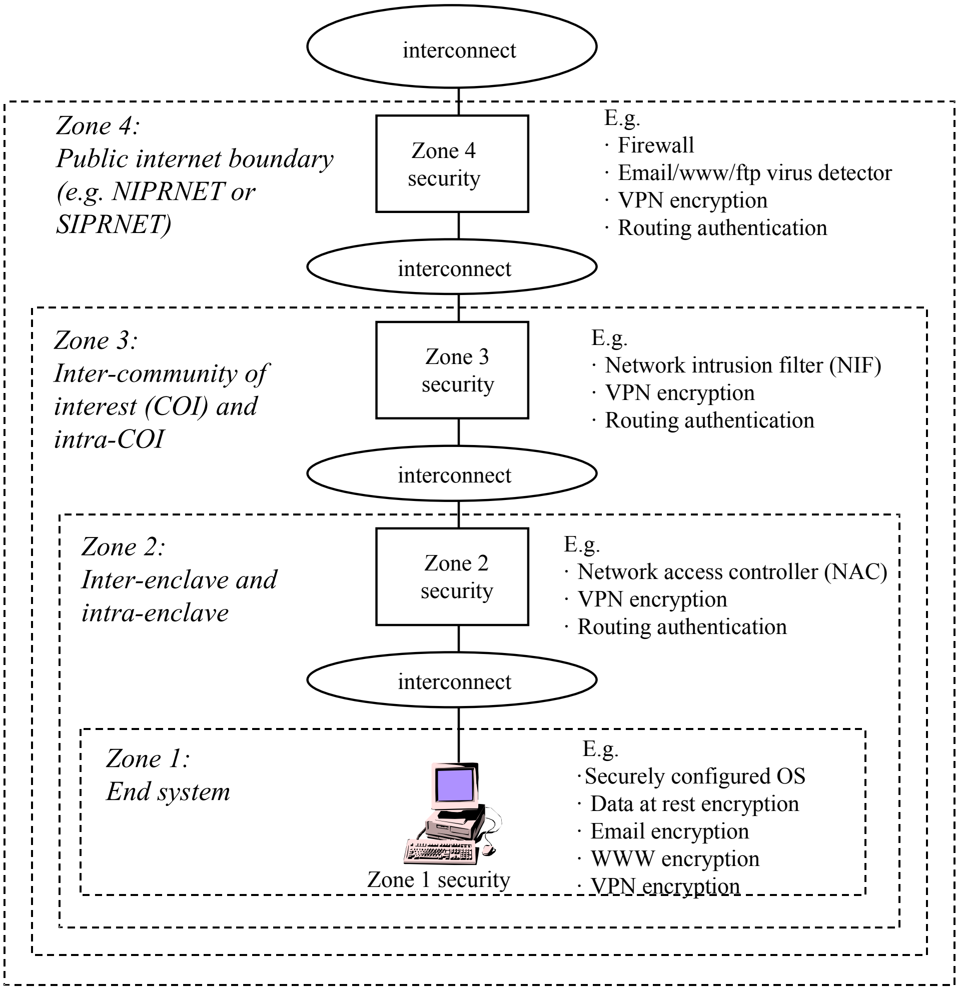


Figure E-1. Generic Framework for Defense in Depth

The defense in depth information protection concept shown in Figure E-1 is directly analogous to naval sea control concepts. Fleet air defense is a representative example. The outer zone is defended by intercept fighters such as F-14s and controlled by E-2Cs. A second layer of defense is the missile zone defended by Aegis cruisers which intercept attackers that are not defeated in the outer layer. Inside the missile zone are the point defense zones where the defensive weapons include chaff, close-in warfare systems, and tactical electronic warfare machinery. Because of the additive effectiveness of these layers, the number of "leakers" that penetrate to the inner zone is less than the capacity of the point defense weapons.

In the Figure E-1 framework, four security layers are defined in the generic framework for defense in depth. The zones of defense may be logical and not necessarily physically separate. Each of the four layers includes appropriate information protection mechanisms selected from the six categories of protection mechanisms and which are required to build secure DON information systems. The most critical of these components is PKI required to support identification and authentication mechanisms and encryption mechanisms that can be applied in the four separate zones.

Figure E-2 summarizes how information protection mechanisms (lower level of granularity derived from section E.2.2) are applied to each architecture security zone and information dimension. A collection of these mechanisms is used to establish the protection needed at each zone. A more in-depth discussion of each information protection mechanism (including appropriate standards guidance) can be found in Chapter 3 of the DON ITSG.

Mechanisms	Info System	Info Domain	Info Content	ZONE			
				1	2	3	4
Bulk, Link, Source Encryption	C,I,a	C,I,a	C,I,a				✓
VPN Encryption	C,I,a	C,I,a	C,I,a	✓	✓	✓	✓
Data at Rest Encryption		C,I,a	C,I,a	✓			
WWW Encryption		C,I,a	C,I,a	✓			
Email Encryption			C,I,a,N	✓			
Digital Signatures			C,I,a,N	✓			
Routing Table Authentication	A,a	A,a			✓	✓	✓
Public Key Infrastructure		☑	☑	☑			
Network Firewall	C,I,A,a	C,I,A,a			○	○	✓
Network Intrusion Filter	C,I,A,a	C,I,A,a			○	✓	○
Network Access Controller	C,I,A,a	C,I,A,a			✓		
Content Security Checking		I,A	I,A	✓	○	○	✓
Operating System Security	C,I,A,a	C,I,A,a	C,I,A,a	✓			
Operating System Configuration	C,I,A,a	C,I,A,a	C,I,A,a	✓			
Password Service	a	a	a	✓			✓

C confidentiality
I integrity
A availability

a authenticity
N non-repudiation

✓ applicable ○optional
☑ infrastructure component

Figure E-2. Application of Information Protection Mechanisms to Zones

E.4 Mechanisms

A collection of security mechanisms is used to establish the protection needed at each zone for each information protection dimension. These are applied in the four zones that comprise the Defense in Depth information security strategy for DON.

E.4.1 Zone 4 Mechanisms

Zone 4 information protection mechanisms are employed at the boundary between the DON enterprise and a public internetwork (e.g., NIPRNET and SIPRNET). These mechanisms are most likely located in an ITSC or supporting facility such as a firewall facility (FWF).

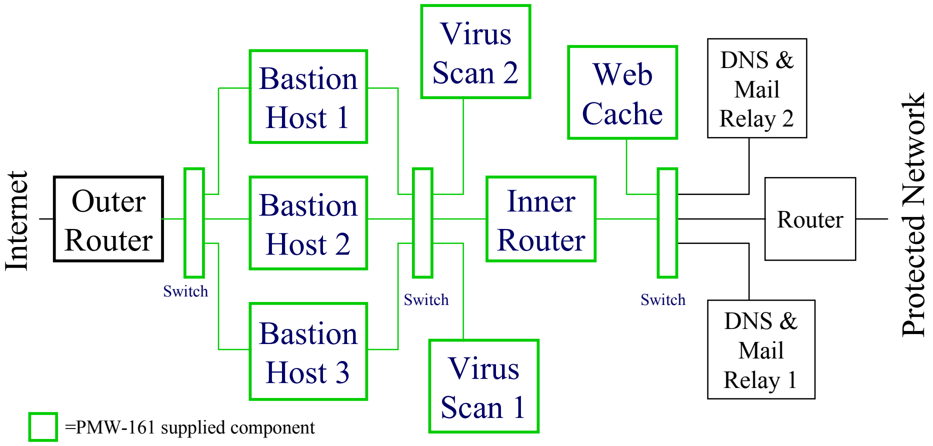
E.4.1.1 Zone 4 Mechanism - Network Firewall

The primary Zone 4 information protection mechanism is the network firewall. The network firewall forms the boundary between the networks under positive Naval control (e.g., regional MANs) and networks not under Naval control (e.g., the NIPRNET/Internet and SIPRNET). This firewall selectively allows external entities to pass information to systems inside the Naval enterprise while blocking many potential attacks (including content security checking or detection of viruses in incoming e-mail attachments and file downloads).

Unprotected modem access defeats the purpose of the firewall and shall be disallowed inside this zone.

Network firewalls should be installed at all gateways to the Internet, NIPRNET, and SIPRNET. These gateways will be located at FWFs, which can be located in ITSCs and/or at other locations within a region for redundancy.

A typical network firewall is the Naval Firewall Security System (NFSS) depicted in Figure E-1. NFSS provides redundant bastion host firewalls, virus checking servers, and a Web cache.



- Parallel Bastion Hosts
- Integrated Virus Checking
- Split DNS
- Mail Storage and Forwarding
- Web Cache
- Identical System for SIPRNET

Figure E-1. Naval Firewall Security System

E.4.1.2 Zone 4 Mechanism – Content Security Checking

E-mail attachments, downloaded files, and comparable items should be automatically checked for viruses as they enter the Naval enterprise from the Internet, NIPRNET, and SIPRNET. This check should be performed as part of the network firewall function.

E.4.1.3 Zone 4 Mechanism – Virtual Private Network (VPN) Encryption

VPN encryption can be used to provide confidentiality and integrity for data transmitted across a public internetwork. Additionally, VPN encryption can provide authentication of the remote system that encrypted the data. When integrated into a suitable system architecture, VPN encryption allows secure “tunnels” to be established across a non-secure internetwork. This allows a private intranet to run securely over a public Internet.

When Naval customers can only connect to ITSCs via the Internet, NIPRNET, or SIPRNET, COTS VPN encryption should be used. This encryption should use the standards set forth in section 3 of the ITSG. This VPN encryption should be integrated with Zone 4 network firewalls.

In addition, connections to classified external networks (e.g., the SIPRNET) must be VPN-encrypted if they are not encrypted using NSA-approved bulk encryptors. This VPN encryption must be performed using an NSA-approved in-line network encryptor (INE). The selection of this device must be coordinated with the owner of the destination network (e.g., DISA) and with CNO N643 for requirement validation and central procurement.

E.4.1.4 Zone 4 Mechanism – User Authentication

Under certain circumstances, non-DON users may require access to internal information services (e.g., an FTP server). Additionally, Naval users may sometimes need to connect back to internal information services from external networks (e.g., while on travel and connecting from a contractor LAN). At a minimum, a one-time encrypted password scheme should be implemented as part of the network firewall to authenticate users requesting such access. As an alternative, SSL with X.509 client certificates may be used to authenticate users to either the network firewall or directly to a secure web server hosted inside the network firewall.

E.4.1.5 Zone 4 Mechanism – Intrusion Detection System

An intrusion detection system (IDS) can detect a wide variety of known network attacks by monitoring network traffic and looking for signatures of known attacks. The Fleet Information Warfare Center (FIWC) has the capability to centrally monitor reports from a commercial IDS known as NetRanger. It is expected that NetRanger will be used to establish a DON centrally-monitored intrusion detection capability. NetRanger IDS sensors should be installed together with network firewalls to detect intrusion incoming from the Internet, NIPRNET, and SIPRNET. These sensors should be installed outside the network firewall to enable FIWC to detect potential attacks that are blocked by the network firewall.

E.4.1.6 Zone 4 Mechanism – Bulk (line) Encryption

Connections to classified external networks (e.g., the SIPRNET) must be bulk-encrypted if they are not already VPN-encrypted using an NSA-approved INE. An NSA-approved bulk encryption device must be used. The selection of this device must be coordinated with the owner of the destination network (e.g., DISA) and with CNO N643 for requirement validation and central procurement.

E.4.1.7 Zone 4 Mechanism – Routing Table Authentication

Routing information exchanged with NIRPNET and SIPRNET core routers (under DISA control) should be authenticated with keyed MD5 where possible. This reduces the possibility that an IP route spoofing attack could be used to disrupt NIPRNET or SIPRNET service. The implementation of keyed MD5 routing protocol authentication for NIPRNET and SIPRNET connections must be coordinated with DISA.

E.4.1.8 Zone 4 Mechanism – ATM Address Filtering

Address filtering is another security technology at the boundary between the DON enterprise ATM network and a public or shared WAN network (DISN ATM WAN, Internet, NIPRNET, etc.). Address filtering is used to allow connections to be made only to and from particular trusted addresses and thus precludes general connectivity. However, in the absence of a PKI, it is not clear that address spoofing can be prevented.

E.4.1.9 Zone 4 Mechanism – ATM Cell Payload Encryptors

ATM cell payload encryptors are becoming available, but interoperability between vendor offerings is not likely.

E.4.1.10 Zone 4 Mechanism – Contractor Network Connections

Extending the Naval intranet (WAN, MAN, CAN, or LAN) to a contractor site may introduce new opportunities for security compromise because the contractor site is outside the Naval physical security perimeter. If the connection to the Naval infrastructure is established outside the security perimeter, then no additional security is required. If, however, the requirement is to penetrate the security infrastructure, then it must be done in a manner that does not weaken or compromise the overall security architecture.

When non-Naval networks connect to the Naval intranet inside the firewall, the following issues must be addressed:

- Does the contractor site connect to other networks? If so, these will constitute back-door connections and the connection should not be allowed.
- Can the contractor network be segmented so that one segment is a separate network without back-door connections? If so, this provides adequate protection and enables satisfactory connection to the Naval infrastructure. This segmentation may not be a desirable option for the contractor site.
- Does the contractor site have adequate controls of physical access? For example, are there locked doors? Who is allowed access to the protected network? What are the policies and procedures for establishing a connection to the protected network? Who can use the workstations that are connected to the physical network?

The Naval intranet will provide external access using VPN technology. This allows access to the Naval intranet from anywhere on the global Internet by establishing a secure tunnel through the Internet to the Naval intranet. Access can be controlled by use of an identity certificate provided by the Naval/DoD Public Key Infrastructure (PKI) solution (described in the next chapter). Using PKI, access to the Naval intranet is controlled on an individual basis instead of at the network or device level. Access to the Naval intranet is granted only to those individuals who have a recognized need for network access. Authorized users must still be authenticated to gain access to systems and applications on the network just like any other Naval user.

This VPN solution provides a general solution for contractor access, as well as for anyone (including Naval personnel who travel and/or telecommute) who requires access from outside of the Naval intranet. In this manner, direct connections can be established from outside the security perimeter while preserving the integrity of the security architecture.

E.4.2 Zone 3 Mechanisms

Zone 3 information protection mechanisms are employed to provide optional security protections to high value information, organizations, or CoIs. These mechanisms may be installed at the

ITSC or the campus ITOC. Although DON enterprise network resources are protected with Zone 3 mechanisms, hosts and network devices controlled by individual commands and/or CoI must implement their own Zone 3 protection mechanisms, but do not establish security policy for organizations/CoIs.

E.4.2.1 Zone 3 Mechanism – Network Intrusion Filter

The Network Intrusion Filter (NIF) provides an optional level of boundary level protections between an organization or CoI and the rest of a region. This allows for high value assets to be afforded additional protections and/or for CoIs to implement more restrictive security polices than the rest of a region. An NIF is essential when connecting fleet teleports to a region if a network firewall is not in place at the teleport. NIFs may be constructed using bastion host firewalls, stateful monitoring firewalls, tightly configured filtering routers, or intrusion detection systems with active shunning capabilities. NIFs may be used to implement VPN encryption to allow a CoI to be distributed across a region or the enterprise.

E.4.2.2 Zone 3 Mechanism – VPN Encryption

VPN encryption is normally implemented using a NIF if required at Zone 3.

E.4.2.3 Zone 3 Mechanism – IDS

IDS may be optionally applied at the boundary between an organization or CoI and the rest of a region. This IDS should be centrally monitored (see Zone 4). Centrally-monitored intrusion detection is considered essential for fleet teleports.

E.4.3 Zone 2 Mechanisms

Zone 2 information protection mechanisms provide boundary protections between a campus LAN and the MAN or region as well as protections on the campus LAN. These protections are normally installed on LANs.

E.4.3.1 Zone 2 Mechanism – Network Access Controller

A network access controller provides a basic level of access control over network connections based on a site/enclave's local security policy. These controls could include restrictions on incoming connections as well as connections between LAN segments internal to the site/enclave. These restrictions could be based on the source and destination addresses of the IP packet as well as the service type (e.g., SMTP e-mail, telnet, HTTP). A NAC should be implemented using the organic filtering IP routers used to connect the site/enclave to the external world. For ATM systems featuring "cut-through" routing, ATM switches should use NSAP filters to ensure all incoming packets are routed to the NAC for security filtering.

E.4.3.2 Zone 2 Mechanism – VPN Encryption

VPN encryption is normally implemented using a NAC if required at Zone 2.

E.4.3.3 Zone 2 Mechanism – Routing Table Authentication

IP routers internal to the DON enterprise should be configured to use keyed MD5 authentication for routing updates. See Zone 4.

E.4.4 Zone 1 Mechanisms

Zone 1 information protection mechanisms provide the inner-most layer of defense for information systems. The protections are implemented on the actual end systems, including NT workstations, NT servers, UNIX servers, and mainframes. Zone 1 information protection includes such mechanisms as secure configurations, data-at-rest encryption, and e-mail encryption. Although DON enterprise network resources are protected with zone 1 mechanisms, individual organizations and/or COI must implement their own zone 1 protection mechanisms.

E.4.4.1 Zone 1 Mechanism – Secure Operating Systems with Secure Configurations

The innermost layer of a defense in depth information protection approach is the computer operating system itself. Selection of operating systems for security features and the correct configuration of those features in an operational environment is critical. Guidance on the selection and configuration of securable operation systems is provided in Section 3.4.4.1 of the ITSG.

E.4.4.2 Zone 1 Mechanism – Content Security Checking

Viruses remain a significant problem for maintaining good information protection. DON information systems should use COTS virus protection software at servers and end user workstations. See Section 3.4.4.6 of the ITSG for further information.

E.4.4.3 Zone 1 Mechanism – E-Mail Encryption

COTS e-mail encryption can be used to provide user-to-user confidentiality, integrity, and authentication. Coupled with a properly managed Public Key Infrastructure (PKI), e-mail encryption can support CoI separation inside the enterprise, a region, a building, or even a workstation. See Section 3.4.4.3 of the ITSG for details.

E.4.4.4 Zone 1 Mechanism – World Wide Web (WWW) Encryption

COTS web encryption can be used to enforce user authentication and access control to information stored on a web server as well as to provide confidentiality, integrity, and authentication for information as it traverses a network. Coupled with a properly managed PKI, web encryption can support CoI separation inside the enterprise, a region, a building, or even a workstation. See Section 3.4.4.4 of the ITSG for details.

E.4.4.5 Zone 1 Mechanism – VPN Encryption

COTS VPN encryption can be used to provide confidentiality, integrity, and authentication for information as it traverses a network. Coupled with a properly managed PKI, VPN encryption can support CoI separation inside the enterprise, a region, or a building. See Section 3.4.4.5 of the ITSG for details. VPN protected modem access is acceptable.

E.4.4.6 Zone 1 Mechanism – Data at Rest Encryption

COTS data-at-rest encryption can be used to provide confidentiality and integrity for information stored on a workstation or server. See Section 3.4.4.2 of the ITSG for details.

E.5 Infrastructure Security Components

In addition to the information protection mechanisms located in the various zones, certain infrastructure components are required to build secure DON information systems. These components include a secure Domain Name System (DNS), Public Key Infrastructure (PKI), network management security support, and network security configuration management systems.

E.5.1 Infrastructure Mechanism – Secure Domain Name System

DNS is essential to the operation of most networked computers and applications. A secure DNS should be installed in ITSCs to reduce the potential of Naval systems being adversely affected by DNS attacks or misconfigurations of DNS servers outside the DON intranet.

E.5.2 Infrastructure Mechanism – Public Key Infrastructure

PKI is the primary security technology requirement. PKI technology will provide security at connection establishment time, but will not perform as an in-line ATM-level firewall. PKI, by itself, is not an adequate ATM-level security solution, but it is regarded as a prerequisite for a strong, flexible security solution.

E.5.3 Infrastructure Mechanism – Network Management Security

Remote management of network infrastructure components (e.g., routers, ATM switches, and SONET multiplexers) will be essential as DON networks are regionalized. If this remote management cannot be accomplished securely, these networks will be vulnerable to denial of service attacks. The simple network management protocol (SNMP) is often used to remotely monitor network components. It also can be used to remotely configure and control network components. Unfortunately, SNMP relies on a single unencrypted community string to control access to managed devices. As a result, SNMP is extremely vulnerable to community string interception and guessing attacks. The use of SNMP for remote monitoring is acceptable, but the use of SNMP for remote configuration and control should be avoided. At a minimum, user name and password should be used for access control to network components that must be remotely configured and controlled. The use of a COTS token-based access control system is highly encouraged.

E.5.4 Infrastructure Mechanisms – Network Security Configuration Management

As DON networks are regionalized and system administration and support functions are centralized to reduce TCO, it will become increasingly important to be able to quickly and automatically determine the security configuration of remote computers. This will allow system administrators at regional ITSCs to find security bugs in user workstations and ensure that appropriate steps are taken to eliminate these bugs. The use of COTS network vulnerability testing tools and security configuration checking tools by regional ITSC administrators is encouraged.

E.5.5 Infrastructure Mechanisms – ATM-level Security

If ATM service providers, including DISA, support only PVCs (they do not support SVCs) and Naval ATM switches connect directly to the service provider's switches, security would be ensured. In this case, the ATM WAN functions as a VPN. However, since the DISN ATM WAN and some commercial ATM service providers support SVCs, it is necessary to implement ATM-layer security to prevent unwanted access to the DON enterprise intranet. Therefore, access controls, at a minimum, are required. Also, because ATM is a connection-oriented protocol, once an ATM connection is established, no intermediate systems take part in filtering higher-layer information. A virtual channel terminating on an end-system inside the DON intranet will bypass traditional IP firewalls. Thus, even with sufficient ATM access controls, there is no method to filter network layer (e.g., IP) data along the link once it has been established. Doing so would make them packet switches, not ATM switches. Therefore, it is not clear just how, or whether, it might be possible to implement firewalls in an ATM environment.

ATM-layer security is essential for the protection of the DON enterprise network. However, at present there is a clear lack of technical standards for ATM-layer security. The ATM Security Framework 1.0 is intended to provide a common language and structure for future technical standards, but it defines no implementable security protocols or algorithms. Commercial ATM-level security is still immature and where it exists, it tends to be vendor-specific. Because IP-layer attacks represent the greatest opportunity for would-be hackers, a lack of ATM-level security does not increase the overall security threat. This architecture identifies technologies that are expected to provide solutions to the security issues and will be a participant in DoD efforts to resolve ATM-layer security.

E.5.6 Infrastructure Mechanisms – IP Security

Network security above the ATM level includes IP security and application security. Although this architecture prescribes ATM to the campus and enables end-to-end (desktop-to-desktop) ATM, classical LANs and IP capabilities will continue to be supported. Therefore, enterprise-wide IP security components are required.